[143] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre Attacks: Exploiting Speculative Execution," *meltdownattack.com*, 2018.

[144] M. Schwarz, C. Maurice, D. Gruss, and S. Mangard, "Fantastic Timers and Where to Find Them: High-resolution Microarchitectural Attacks in JavaScript," in *Financial Cryptography and Data Security - 21st International Conference, FC*, vol. 10322, pp. 247–267, 2017.

[145] G. J. Duck, X. Gao, and A. Roychoudhury, "Binary Rewriting Without Control Flow Recovery," in *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI*, pp. 151–163, 2020.

[146] J. D. Seideman, *Transformation and Abstraction to Aid Comparison of Binary Executables Across Compilation Environments.* PhD thesis, City University of New York, 2023.

[147] H. Huang, A. M. Youssef, and M. Debbabi, "BinSequence: Fast, Accurate and Scalable Binary Code Reuse Detection," *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017.

[148] J. Jang, A. Agrawal, and D. Brumley, "ReDeBug: Finding Unpatched Code Clones in Entire OS Distributions," in *2012 IEEE Symposium on Security and Privacy*, pp. 48–62, 2012.

[149] H. Jang, K. Yang, G. Lee, Y. Na, J. D. Seideman, S. Luo, H. Lee, and S. Dietrich, "QuickBCC: Quick and Scalable Binary Vulnerable Code Clone Detection," in *ICT Systems Security and Privacy Protection*, pp. 66–82, 2021.

Part II

Included papers